The HIPAA Implementation Newsletter
Issue #56 – Friday, April 25, 2003
| SARS | Identity Theft | Status | Security |
Web format with links at http://lpf.com/hipaa/

The First Newsletter after the Privacy Compliance Date

HIPAA privacy regulations are now in effect. Our local drug store has modified their signs from “Please wait here” to “Please wait here for privacy.” They and a doctor we visited give us the necessary forms and we signed for them. A small additional burden but otherwise business as usual. We subscribe to several listserves and responses range from similar to ours to some horror stories. Given the complexity of the job, we appear to be off to a good start and there is certainly more to do.

SARS Exploitation by Computer Virus
“It's a different kind of SARS virus on the loose: British antivirus company Sophos Plc has issued a warning of a new computer worm that takes advantage of growing concern over the biological SARS virus. Known as W32/ Coronex-A, the mass-mailer worm forwards itself to all contacts in *Microsoft Outlook* address books and attempts to dupe innocent computer users into opening an attachment offering details on the current SARS (Severe Acute Respiratory Syndrome) epidemic.
“‘The worm has been deliberately coded to exploit the public's genuine concern about SARS, and is just a further demonstration of the ways that virus writers attempt to use psychological trickery to spread their creations,’ said Charles Cousins, managing director of Sophos Anti-Virus Asia. ‘It is important that people call this virus by its proper name, Coronex, rather than 'the SARS virus'. If they don't it will only add to the confusion and panic.”
+ More at: http://star-techcentral.com/tech/story.asp?file=/2003/4/24/technology/24sarsvirus&sec=technology
+ And: Symantec (Norton Anti-Virus software)
http://securityresponse.symantec.com/avcenter/venc/data/w32.coronex@mm.html
Symantec has it rated as a low risk but distribution is now high. It was just discovered on April 21.

Identity Theft: Visa Goes Beyond Technical Security

“Visa USA today (April 22, 2003) announced a national initiative to assist identity theft victims in recovering from the aftermath of the crime. According to Visa research, 68 percent of identity theft victims say the biggest problem they face is the time it takes to remedy the situation. Victims often cite efforts such as correcting inaccurate credit reports, requesting a new Social Security number and closing card account numbers as time consuming. Today's announcement builds on Visa's industry leading consumer protections and fraud prevention, such as its zero liability policy for cardholders.

“Through a unique partnership with Call For Action, a consumer network based in Maryland, victims of identity theft can receive free, confidential counseling by calling 1-866-ID-HOTLINE. … ‘This partnership gives consumers a number of valuable resources to protect themselves from identity thieves, but more importantly, it offers them a place to turn when they've been victimized,’ said Carl Pascarella, president and CEO of Visa USA.

“Visa also announced today that it is offering Personal Identity Theft Coverage as a new optional benefit for Visa cardholders. Member financial institutions will have the opportunity to purchase this coverage to offer free to their cardholders. The insurance coverage goes beyond Visa's zero liability policy by providing eligible cardholders with coverage ranging from $1,000 to $15,000 in reimbursement for lost wages, legal fees and other costs associated with recovering from identity theft. Coverage amount is determined by the member financial institutions.”
+ More at:
http://www.usa.visa.com/personal/about_visa/newsroom/press_releases/nr157.html

Identity Theft: Survey

“Nine out of 10 Americans (92 percent) think it is important that the government take action on the issue of identity theft, the nation's fastest growing crime, according to a new survey released by Star Systems. The survey, conducted for STAR in April 2003, gives the latest picture on the threat of identity theft to American consumers, businesses and financial institutions. In the survey, 5.6 percent of the respondents replied ‘yes’ when asked whether they had ‘ever been the victim of identity theft…’ An earlier STAR survey, conducted in November 2002, found a similar percentage, 5.5 percent. Close to 51 percent of Americans are very concerned about identity theft, significantly more than unemployment.”
+ More at: http://www.star.com/cfm/news-press.cfm?id=81

Status: Transactions, WEDI

“WEDI has assessed potential impacts of non-compliance with the HIPAA TCS standards and believes that they are significant, particularly disruption of business transactions and payments. This assessment is based on anecdotal evidence from a representative cross-section of the healthcare industry, which indicates that a substantial number of covered entities and several states, such as New Jersey1, are not now sufficiently enabled to achieve a state of compliance with HIPAA TCS standards by October 16, 2003. Quantitative estimates are difficult to construct. However, to give an order of magnitude to the problem, even if 95% of current electronic claims submitters were ready and in production with their current trading partners on October 16, 2003, the cost and the cash flow delays associated with the remaining 5% would have an adverse impact on the healthcare industry.

“If WEDI’s assessment is correct - and WEDI believes that it is - then providers and health plans would be forced by HIPAA to revert to paper submission to avoid non-compliance. Should any material reversion to paper be the only option for compliance, WEDI believes that providers and health plans would expend significant time, resources, and money that could be more productively allocated to ensuring a successful HIPAA TCS standards implementation. For many health plans, resources, personnel, and time necessary to gear up for an avalanche of paper would not be available. In short, payments to providers would be seriously disrupted, affecting providers nationwide.”

The letter and attachments suggest a number of ways to reduce the risk and assure that available resources are used to get to compliance.
+ More at:
http://www.wedi.org/cmsUploads/pdfUpload/commentLetters/pub/Letter_to_Sec_Thompson_pdf.pdf

Status: Transactions and States

“We conducted telephone interviews with officials from the 51 state Medicaid agencies (50 states and the District of Columbia). While few similarities exist in the planning and strategies among the 51 Medicaid agencies, 42 programs (approximately 80 percent) anticipate that they will be in compliance by October 2003. Of the remaining nine programs, eight are developing contingency plans to allow them to conduct business with compliant and noncompliant trading partners, and the ninth is expected to be minimally compliant by the deadline, with expectations that a new compliant system will be on line by March 2004.” HIPAA Readiness: Administrative Simplification For Medicaid State Agencies Office of Inspector General
+ More at: http://oig.hhs.gov/oei/reports/oei-09-02-00420.pdf

Security: Audits

“‘Security audits can be used by security administrators and officers to improve or verify their work, but audits can hurt if admins aren't savvy about the process’ said Roeland Stouthard, a former auditor with KPMG Information Risk Management. External audits can have many facets. Auditors may do ethical hacking to test systems and networks. They may also review projects to make sure they are meeting objectives. Tools and applications being used by an enterprise may also be scrutinized. Source-code reviews of homegrown applications can also be on the agenda.

“For Paul Bergman, director of IT for Maxygen Inc., a biotech firm, external audits are a way of ‘closing loopholes’ within the company's infrastructure and do not pose a threat. His company doesn't have the internal expertise to double-check its security, so auditors provide a verification of their work.

“Security staffers should prepare for audits by becoming aware of the auditing process -- something that, in some cases, could enable them to influence the outcome, expose security issues or push a particular agenda through. Security managers shouldn't be intimidated by auditors. In fact, auditors like it when you challenge them, because it shows you really care about your work and processes. ‘No one has carte blanche. Auditors tend to ask for more information than they need,’ Stouthard said, noting that making auditors explain why they are requesting information makes for a better audit.

“Managing expectations is another way of ensuring that the audit goes well. Staff should be aware of the kinds of things auditors are looking to learn from them. For example, if a project manager is talking about everything from money to deadlines to managing risk that could set off some warning lights. ‘The auditors may look to see if the plans are too detailed.’

“Of course, showing auditors how some things are running well should be a goal. But letting auditors know about weaknesses has its advantages as well. For example, security staff could highlight certain problems that they know the company has and suggest solutions. These could end up in the auditor's final report, which is usually given a fair amount of attention and weight by management.

“Once the auditors' report comes out, there are few things a security manager can do to influence the outcome. Things they should look for are recommendations that are too

vague or too concise; auditors are not implementation specialists. So if a report casually recommends a single sign-on project that could cost $1 million, then that should set off warning lights. Sometimes, there is an opportunity for a manager to submit a written reaction to the audit. But this is not the place to be negative or nitpicky, Stouthard said. 'Don't whine in the reaction, as it will live on [long after the details of the audit are forgotten]."
+ More at:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci894590,00.html

Security: Mobile Devices

"Enterprises that do not want to include mobile devices in their environments often use security as an excuse, saying they fear the loss of sensitive data that could result from a PDA being stolen or an unsecured wireless connection used. Such concerns are no longer viable, said Kevin Burden, of International Data Corp. There are technologies available to properly secure mobile devices that are endorsed by the National Security Agency, the CIA and the FBI. 'If they are good enough for them, then they should be good enough for most companies.' For example, there are ways to make devices lock or destroy lost data by sending the machine a special message. Also, some mobile devices have high-powered processors that will support 128-bit encryption.

"Mobile devices do pose unique challenges, from a security prospective. There are some general steps users can take to address them, like integrating security programs for mobile and wireless systems into the overall security blueprint, said Tim Scannell, of Shoreline Research Inc. Here are a few more suggestions from Scannell:

- Implement strong asset management, virus checking, loss prevention and other controls for mobile systems that will prohibit unauthorized access and the entry of corrupted data.
- Investigate alternatives that allow secure access to company information through a firewall, such as mobile VPNs.
- Develop a system of more frequent and thorough security audits for mobile devices.
- Incorporate security awareness into your mobile training and support programs, so that everyone understands just how important an issue security is within a company's overall IT strategy."

+ More at:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci892256,00.html

Security: Mobile Devices for EMS

"First responders in Norwich Township, Ohio, are using wireless devices and database software to get their ambulances back on the road faster as well as to comply with Health Insurance Portability and Accountability Act privacy rules.

"After each ambulance run, EMS workers are required by state law to log a patient care report of vital signs, dispatch time and medical procedures performed en route. The data goes to the hospital staff, the fire department and Ohio health officials. ,,, In the past, EMS workers filled out a paper report, which took about 45 minutes per incident. Then the EMS workers had to give the hospital staff a copy when they transferred the patient. Often they had to take time explaining their special procedure codes to the hospital staff.

"Now EMS crews use an infrared port to beam the data to printers at nine hospitals in Franklin County. 'It prints out in plain English—no codes,' Papa said. That has reduced the time EMS crews spend at the hospital explaining the circumstances. Papa said that's the biggest benefit because it 'gets the emergency vehicles back out on the road as soon as possible, ready to handle the next emergency.'

"When the EMS crew returns to the fire station, they 'cradle sync' the device with larger systems. The data is immediately available for statistical analysis. Before, data would stay on paper for days or weeks before it was keyed into the database. Township officials estimated they have reduced data processing costs by more than 90 percent. The software meets HIPAA regulations for privacy and confidentiality, Papa said."
+ More at: http://www.gcn.com/vol1_no1/daily-updates/21516-1.html

Security: SPAM

"Spam is overtaking viruses as the biggest pain for businesses using the web. Monthly reports for March from antivirus companies show that, while virus activity is experiencing single digit growth, spam is growing at between 10 and 30 per cent and now accounts for one in every 2.8 emails. Whereas a virus infection costs a lot they tend to be isolated occurrences. Spam is like death by a thousand cuts, once you factor in the cost of bandwidth, storage and administration" [and the employee time wasted checking and then deleting it.] "Analysts are predicting that half of all emails will be spam by the end of the year." …
+ More at: http://www.vnunet.com/News/1139934

Security: SearchSecurity HIPAA Expert
Home page and list of questions and answers:
http://searchsecurity.techtarget.com/ateAnswers/0,289620,sid14_cid487134_tax292915,00.html
DSL with NAT firewall:
http://searchsecurity.techtarget.com/ateQuestionNResponse/0,289625,sid14_cid527366_tax292915,00.html
Firewalls for small office:
http://searchsecurity.techtarget.com/ateQuestionNResponse/0,289625,sid14_cid515961_tax292915,00.html
PHI and email:
http://searchsecurity.techtarget.com/ateQuestionNResponse/0,289625,sid14_cid524316_tax292915,00.html

Conferences

We have special interest in banking and HIPAA and have joined the Medical Banking Project. Their **10th HIPAA Policy Roundtable** will be on May 19, 2003. More in future issues.

THE HIPAA SUMMIT WEST will be held June 4-7, 2003 at the Seattle Convention Center & Sheraton Seattle Hotel & Towers in Seattle Washington. The HIPAA Summit West, announced special sessions on HIPAA enforcement and security and a special session at the Microsoft Conference Center in Redmond WA on Saturday, June 7, 2003.
http://www.HIPAASummit.com

The HIPAA Summit Conference Series has announced that the 6th National HIPAA Summit's faculty presentations are available in both PDF and PowerPoint format at no cost at: http://www.HIPAASummit.com

---